Presentation to LFN Developer & Testing Forum

Network Slicing Security Enhancement Security Call Data Records (SCDR)

17-18 November 2022, Seattle, WA.

David Armbrust – MITRE

darmbrust@mitre.org

This technical data deliverable was developed using contract funds under Basic Contract No. W56KGU-18-D-0004

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Agenda ~25 min presentation with 5 min Q&A/feedback

- Defining SCDR
  - Overview
  - Security roles of DCAE, NWDAF, and SCDR - Differentiated Security Focus in network slicing
  - Security Call Data Record – Desired artifacts
- “Operationalizing” SCDR
  - Compatible with 3GPP specifications and architecture
  - Roles of Carriers and CSPs in SCDR generation & delivery
  - Roles of Enterprise networks using analytics for visibility and anomalous NS behavior detection
- Demonstration: proof-of-concept SCDR use case – location anomaly detection
- Summary of benefits

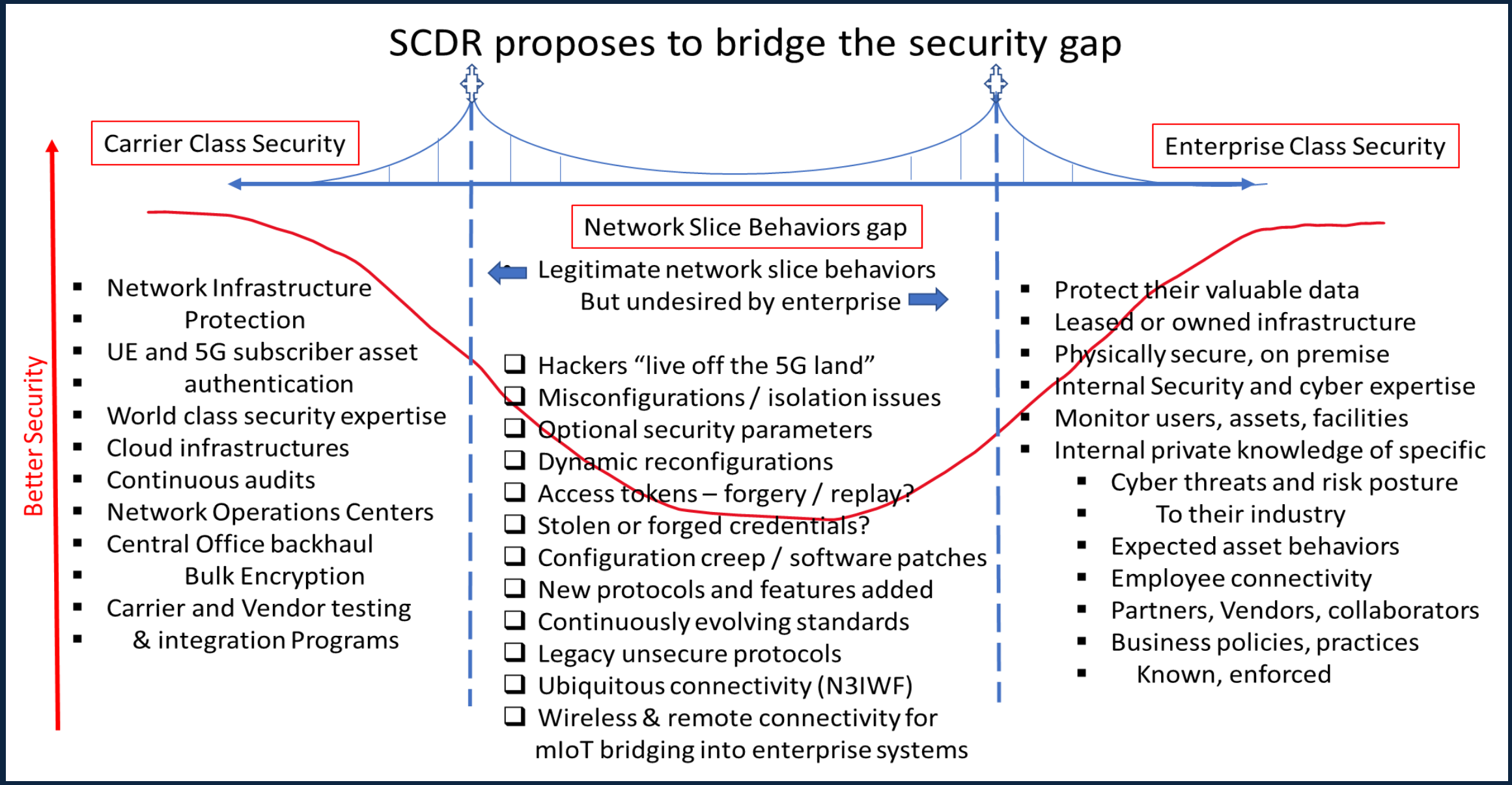
MITRE

SCDR Overview

- 5G Network Slicing (NS) will be a key enabler for companies and enterprise verticals.
- Therefore, Network Slice enterprise Consumers (NSC) will demand *security visibility* and *operational transparency* for every NS instantiation.
- Enhanced security for enterprise verticals (ex. financial, manufacturing, government, etc.) can be achieved by combining operational *data from network slices* and *knowledge from the enterprise*.
- MNOs cannot access internal enterprise knowledge to use this information in MNO security analytics; however, the enterprise can and should receive evidence about the MNO's security posture and operations concerning their purchased network slice instantiation.
- Security Call Data Record (SCDR) is a framework to make this MNO and CSP end-to-end data available and make possible the detection of nuanced and advanced persistent threats using tailored enterprise analytics for assessing their own network slice behaviors.
- This presentation will describe the SCDR framework and show a recorded video demonstration.
  - The use case will focus on the artifacts of an enterprise's UE 5G NS attachment, used to join a network slice from MNO authorized but suspicious 5G connection locations. The analytics will expose anomalous connectivity in the network slice, inconsistent with enterprise knowledge, indicating malicious activity from potentially stolen credentials.

MITRE

SCDR Motivation



Security roles in 5G

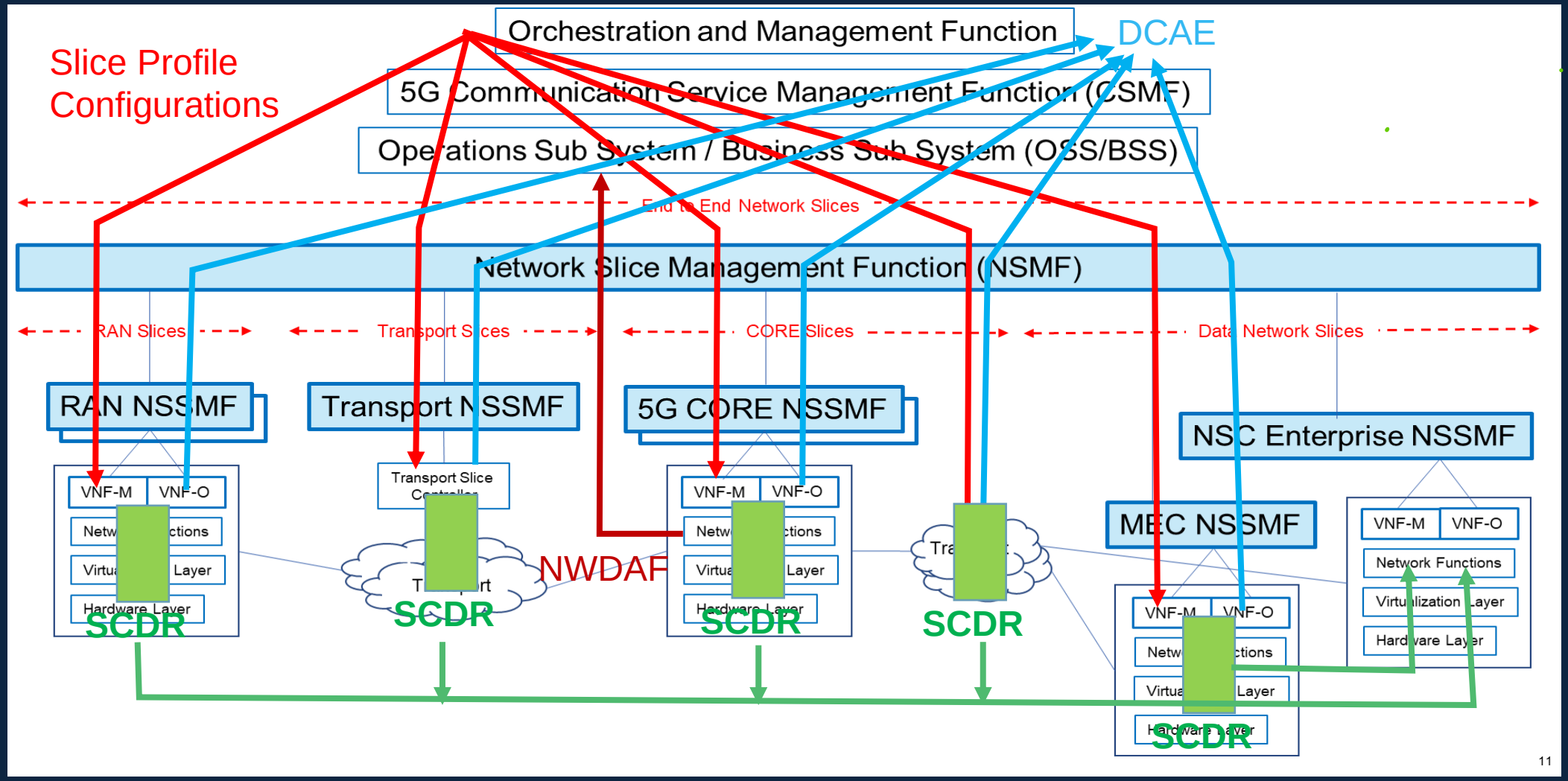
5G Network Slice Provider - Orchestration, Administration, & Management of Network Slices (Ex. ONAP & DCAE)

5G COREs artifact collection, centralization, and security analytics processing for the PLMNs and MNOs (NWDAF)

Proposed: End-to-end Network Slicing behavior artifact collection for Enterprise Consumer (SCDR)

MITRE

Security focus of DCAE, NWDAF, and SCDR



SCDR security context – record details (preliminary)

Subscriber Network Slice Profile configurations →

PLMNs and CSPs Software Bill of Materials (SBOMs) →

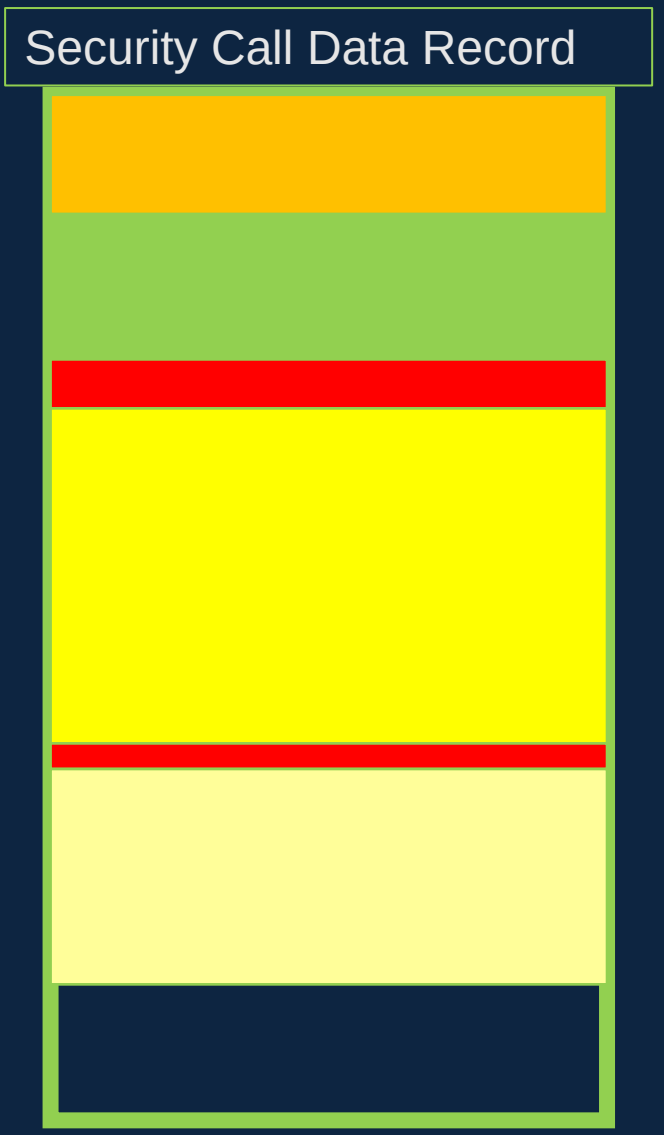
PLMNs and CSPs – Security Posture / Versions / Patch History →

Network Slice UE Connection attributes, etc. →
- Admitted connections
- Dynamic Changes to configurations

CSP detected Network Slice security anomalies →

Network slice operational measurements and statistics →

Customization - TBD selected attributes →
- specific to subscriber's cyber threats



MITRE

“Operationalizing” SCDR

MITRE

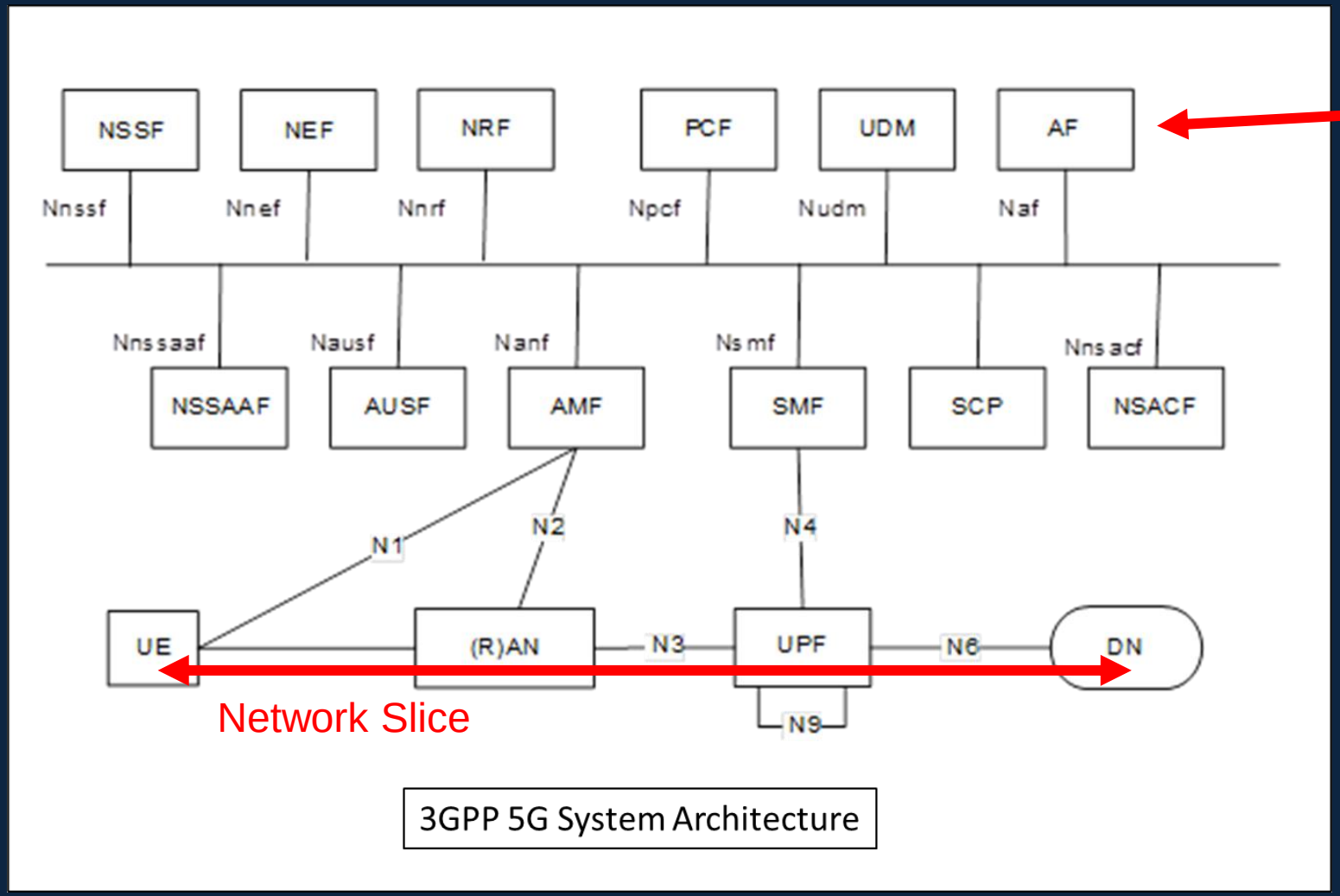
SCDR Operational framework

Three components needed for realization:

1. SCDR-Application Function - Interfaces with 3GPP compliant VNFs to programmatically extract artifacts through APIs and records artifacts in a file on each CSP
2. Subscriber's H-PLMN receives and aggregates all SCDRs from all CSPs involved in NS
   - H-PLMN is an industry trusted intermediary, with authority, to enforce standards compliance
   - SCDR can be Monetized at:
     - Termination of a routine / uneventful active NS
     - Timed intervals – ex. Smart warehouse / hospital - mIoT security augmentation (ex. every hour)
     - Immediately after detected high risk security event – VMs crash, SLA violated, etc.
3. Subscriber uses SCDRs for security visibility and operational transparency into their NS using their tailored security analytics and enterprise knowledge.

MITRE

SCDR compatible with 3GPP architecture & standards

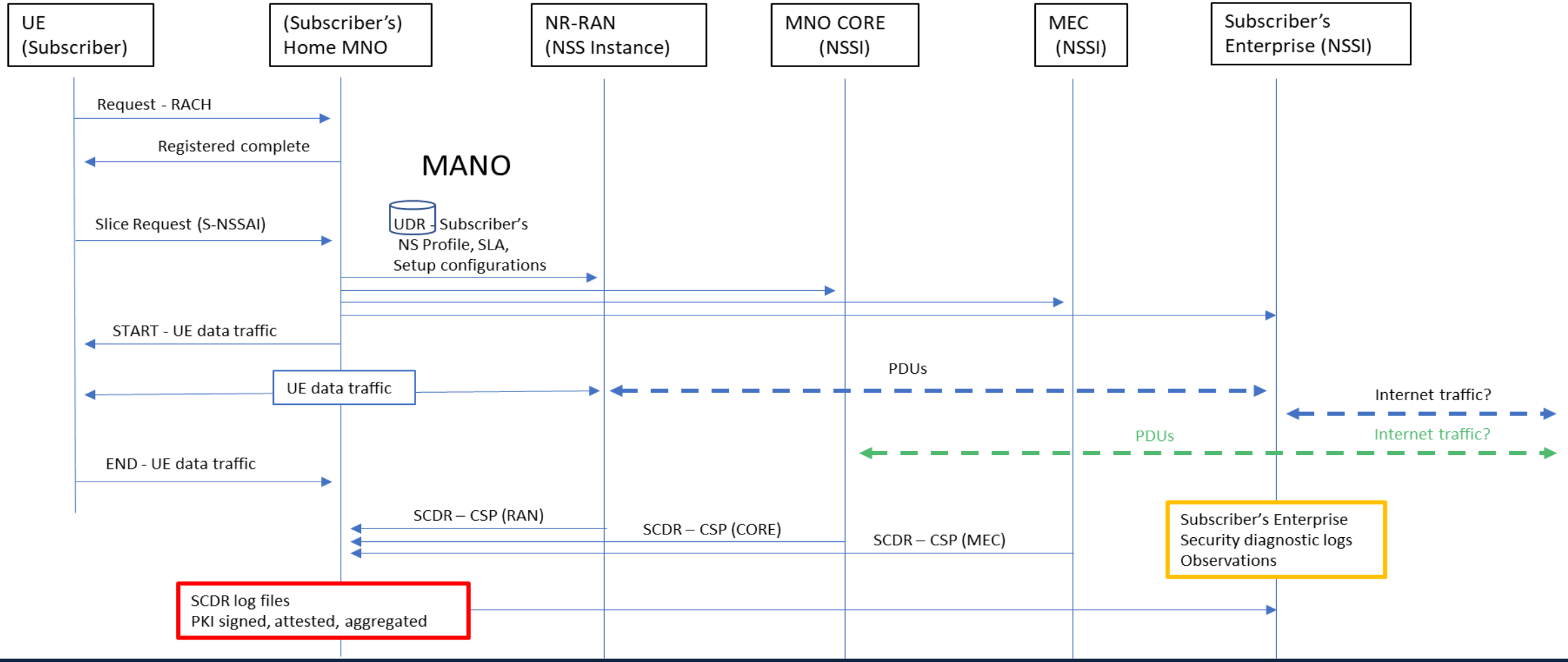


3GPP 5G System Architecture

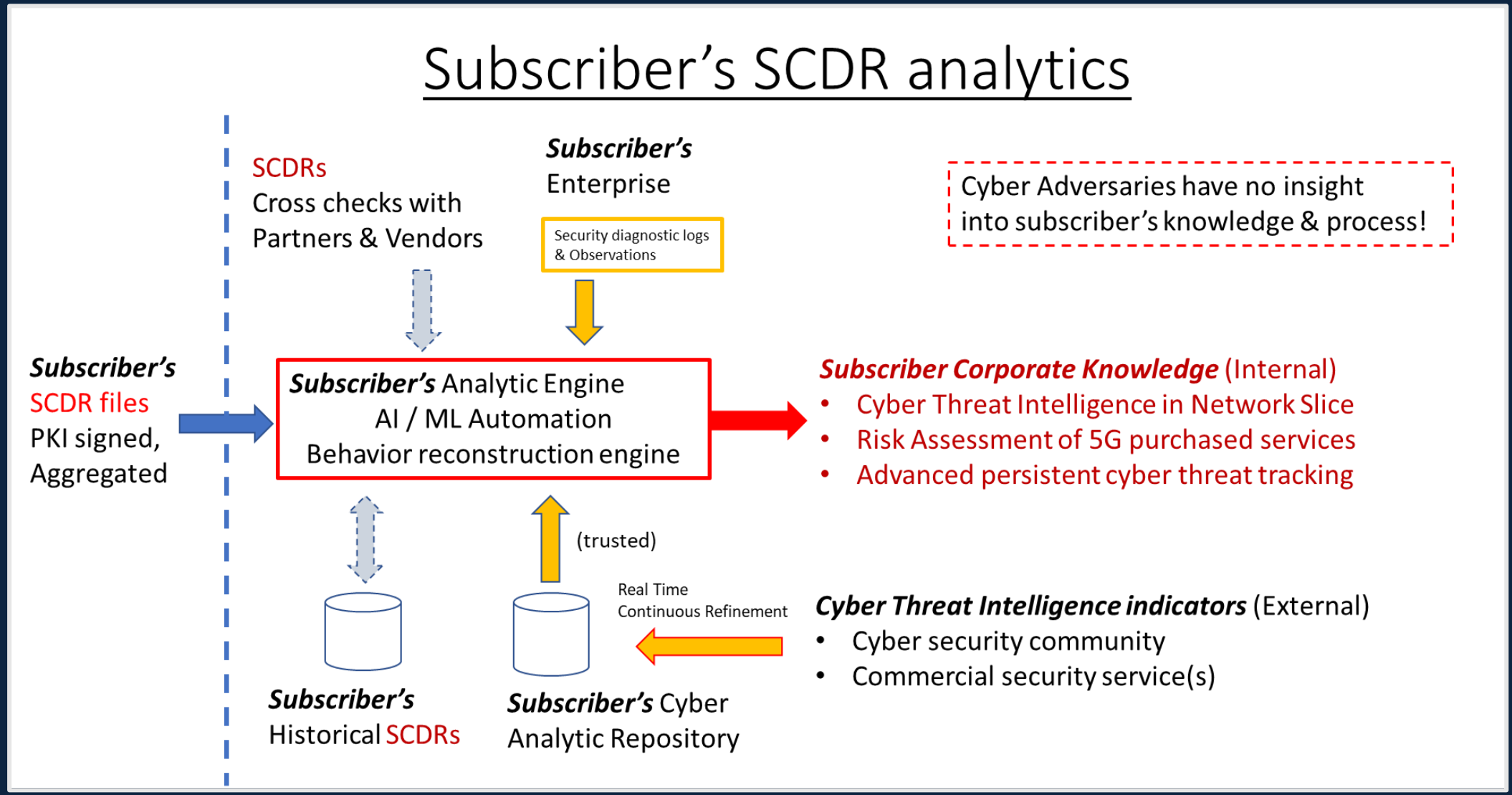
SCDR-AF

3GPP compliant structure with all the rights, privileges, and policies of the infrastructure VNFs and Application Function NFs that operate on, or have access to, the subscriber's Network Slice.

Network Slice subnets: Communications Service providers (CSPs) & SCDRs



Subscriber's Enterprise Security Operations Center (SOC)



MITRE

SCDR demo video using

UERANSIM and OPEN5GS simulators

MITRE

Demo sequence

- Registration, authentication, network slice attachment
- Four legitimate callers connect into their network slice, one caller leaves

  (Absent caller's stolen credentials used to connect from anomalous location)

- Two independent SCDR records are provided to the enterprise
- Enterprise analytics detect an anomaly using the combined SCDRs, public, and private information, and cyber threat intelligence

(leverage UE registration events – extract {timestamp, location, Cell_ID, gNB_ID, SUPI, NS_ID, NCGI)

MITRE

Play demo video

Video Removed due to size

Summary

Significance of SCDR video

- Demonstrate that SCDR concept is feasible
- Demonstrate the value of combined domain knowledge
- SCDR has a 3GPP compliant architecture and leverages existing specifications
- SCDR can be implemented in mature simulators and ported to real testbeds
- Enterprise analytics can greatly enhance security visibility and operational transparency in their network slices
- Tailored analytics focus security on highest risk activities for enterprise verticals and standardize collaboration in security coalitions among partners in vertical industries or military networks

MITRE

Key benefits of SCDR framework

Enterprise verticals can use information exposed by multi-domain SCDR records to enhance their security by identifying suspicious behavior in their network slice.

- Cross Correlating artifacts from different CSPs' SCDRs exposes inconsistencies across the end-to-end Network slice.
- Correlating Enterprise private facts & knowledge against current artifacts in SCDRs utilizes dynamic information not publicity available nor predictable limiting malicious options
- Historical SCDRs allows tracking NS Configuration changes over time
- Enterprise partners can provide SCDRs enabling a stronger security collective among enterprise verticals, partners, vendors, and their customers
- Mutual security benefit for Carriers, MNOs, CSPs, with Enterprise consumers. Together combining each domains unique knowledge to detect and track nuanced malicious behaviors and persistent threats in network slices.

MITRE

Proof-of-concepts – additional use cases

- SCDR enables enhanced security visibility and operational transparency for the enterprise vertical NS consumer.
- If interested, reach out and help us make SCDR a reality.

- - - - - Contact: scdr-list@mitre.org - - - - -

- ✓ 5G enterprise asset(s) - detect geographic *location* inconsistencies?
- ❑ 5G distributed protocols - detect anomalous *latency* issues – connection via TOR, MITM?
- ❑ 5G NS *Isolation* issues - VNF infrastructure access, NS crosstalk access, access tokens?
- ❑ 5G CSP possible NS *routing and connections* manipulation issues, data exfiltration?
- ❑ 5G protocol *race conditions* on a distributed network – temporary open connections?

MITRE

Questions? or Comments!

scdr-list@mitre.org

MITRE

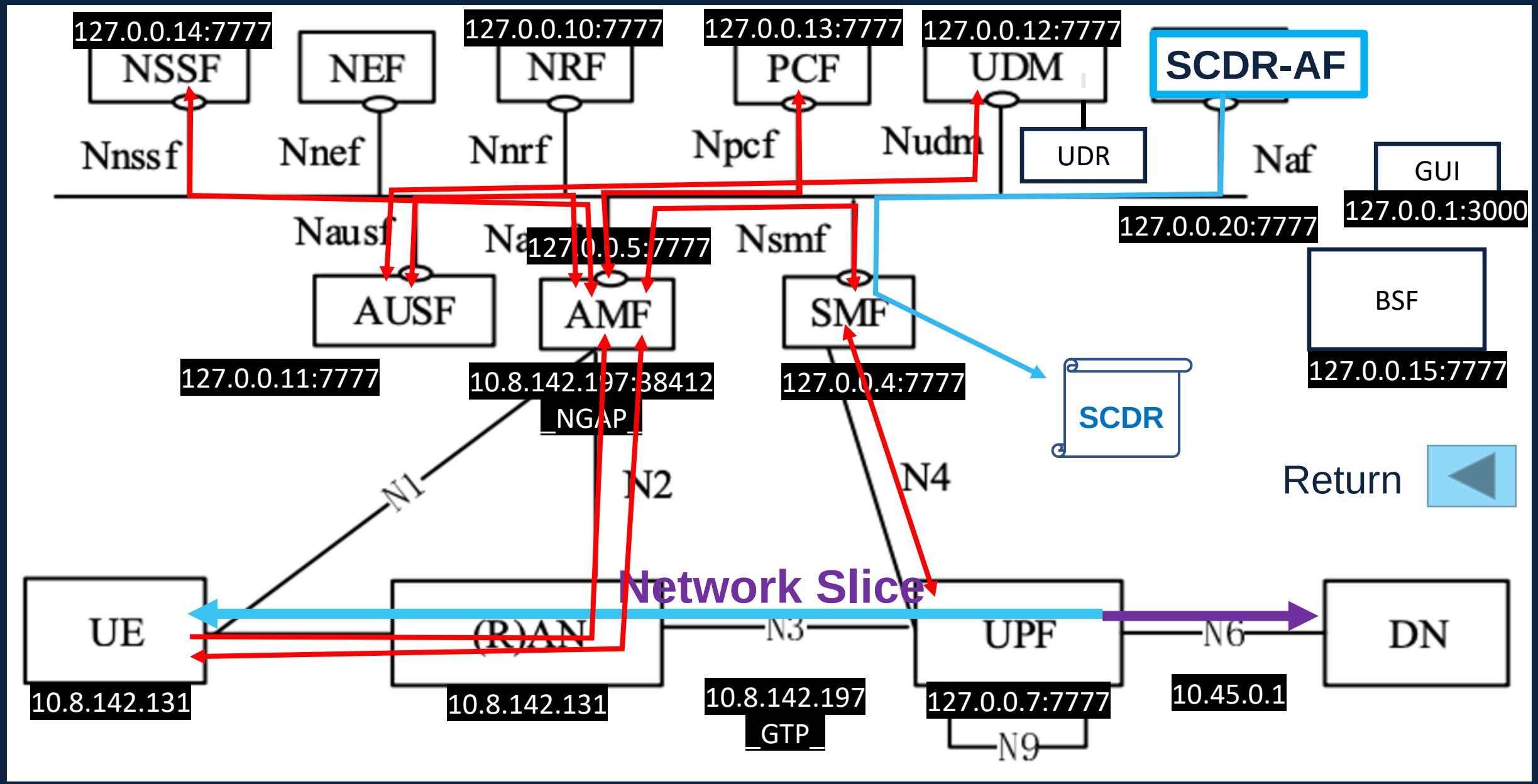
- - - Back up - - -

Animation Slides
and Simulator Config artifacts

MITRE

Click to start

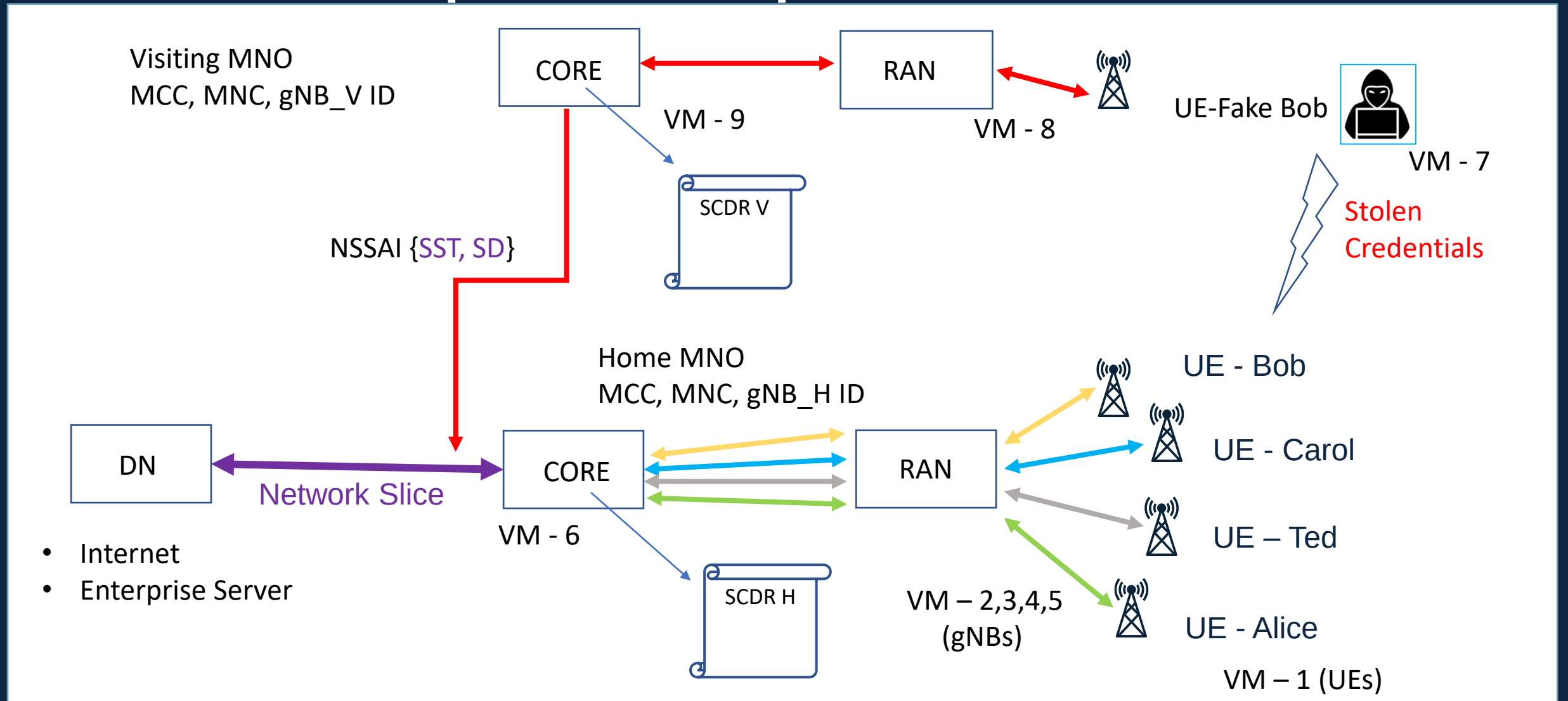
UE registration, network slice admission to DN connection



Click to start

Simulation setup – demo sequence

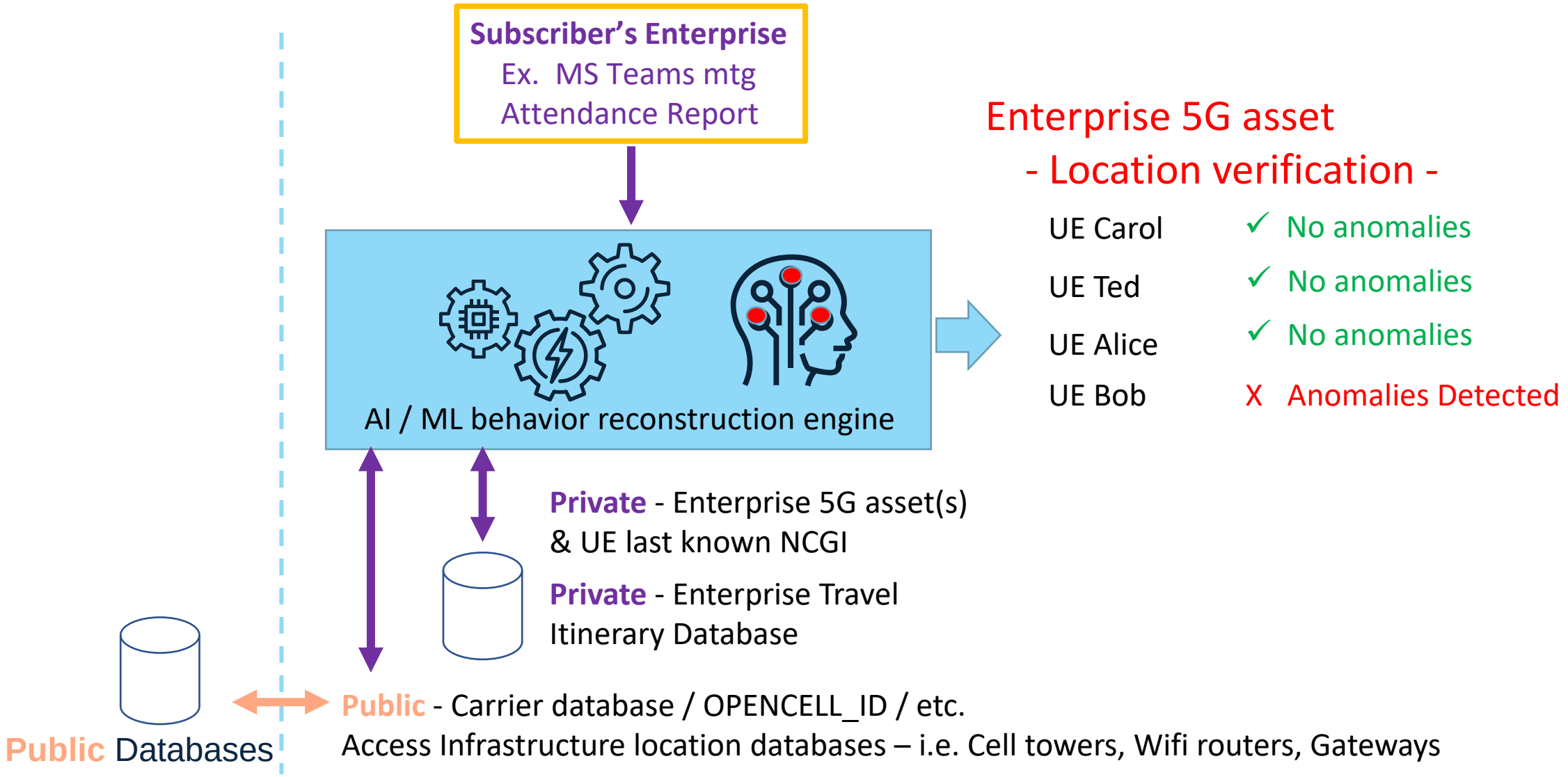
Return



Click to start

Enterprise consumer – tailored analytics

Return



Modified Simulator Configuration Files

- Open5GS

```yaml
amf:
    sbi:
      - addr: 127.0.0.5
        port: 7777
    ngap:
      - addr: 10.8.142.197
    guami:
      - plmn_id:
          mcc: 311
          mnc: 480
        amf_id:
          region: 2
          set: 1
    tai:
      - plmn_id:
          mcc: 311
          mnc: 480
        tac: [14850,27147,26122,29959]
    plmn_support:
      - plmn_id:
          mcc: 311
          mnc: 480
        s_nssai:
          - sst: 1
            sd: 1
```

```yaml
smf:
    info:
      - s_nssai:
          - sst: 1
            dnn:
              - internet
        tai:
          - plmn_id:
              mcc: 311
              mnc: 480
            tac: [14850,27147,26122,29959]
```

```yaml
upf:
    pfcp:
      - addr: 127.0.0.7
    gtpu:
      - addr: 10.8.142.197
    subnet:
      - addr: 10.45.0.1/16
        dnn: internet
```

- UERANSIM

```yaml
# IMSI number of the UE. IMSI = [MCC|MNC|MSISDN] (In total 15 digits)
supi: 'imsi-311480000000001'
# Mobile Country Code value of HPLMN
mcc: '311'
# Mobile Network Code value of HPLMN (2 or 3 digits)
mnc: '480'

# Permanent subscription key
key: '465B5CE8B199B49FAA5F0A2EE238A6BC'
# Operator code (OP or OPC) of the UE
op: 'E8ED289DEBA952E4283B54E88E6183CA'

# List of gNB IP addresses for Radio Link Simulation
gnbSearchList:
  - 10.8.33.15

# Configured NSSAI for this UE by HPLMN
configured-nssai:
  - sst: 1
    sd: 1
```

```yaml
mcc: '311'          # Mobile Country Code value
mnc: '480'          # Mobile Network Code value (2 or 3 digits)

nci: '0x5768D0C'    # NR Cell Identity (36-bit)
idLength: 32        # NR gNB ID length in bits [22...32]
tac: 14850          # Tracking Area Code

# List of AMF address information
amfConfigs:
  - address: 10.8.142.197
    port: 38412
```

MITRE